Ring: Set together with two binary operations so that:

(1) $a+b \in R$

(2) $a+b=b+a$

(3) $(a+b)+c=a+(b+c)$

(4) $\exists\, 0$ s.t. $a+0=0+a=a$

(5) $\exists\, -a$ s.t. $a-a=-a+a=0$

(6) $a \cdot b \in R$

(7) $a \cdot (b \cdot c)=(a \cdot b) \cdot c$

(8) $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$

Commutative: The "multiplication" is commutative.

With Unit: There exists an element, called 1, so that $1 \cdot a=a \cdot 1=a$.

Integral Domain: Commutative ring with no zero divisors.
$(a \cdot b=0,\ a,b \neq 0)$

Division Ring: Non-zero elements are a group under multiplication

Field: Commutative division ring

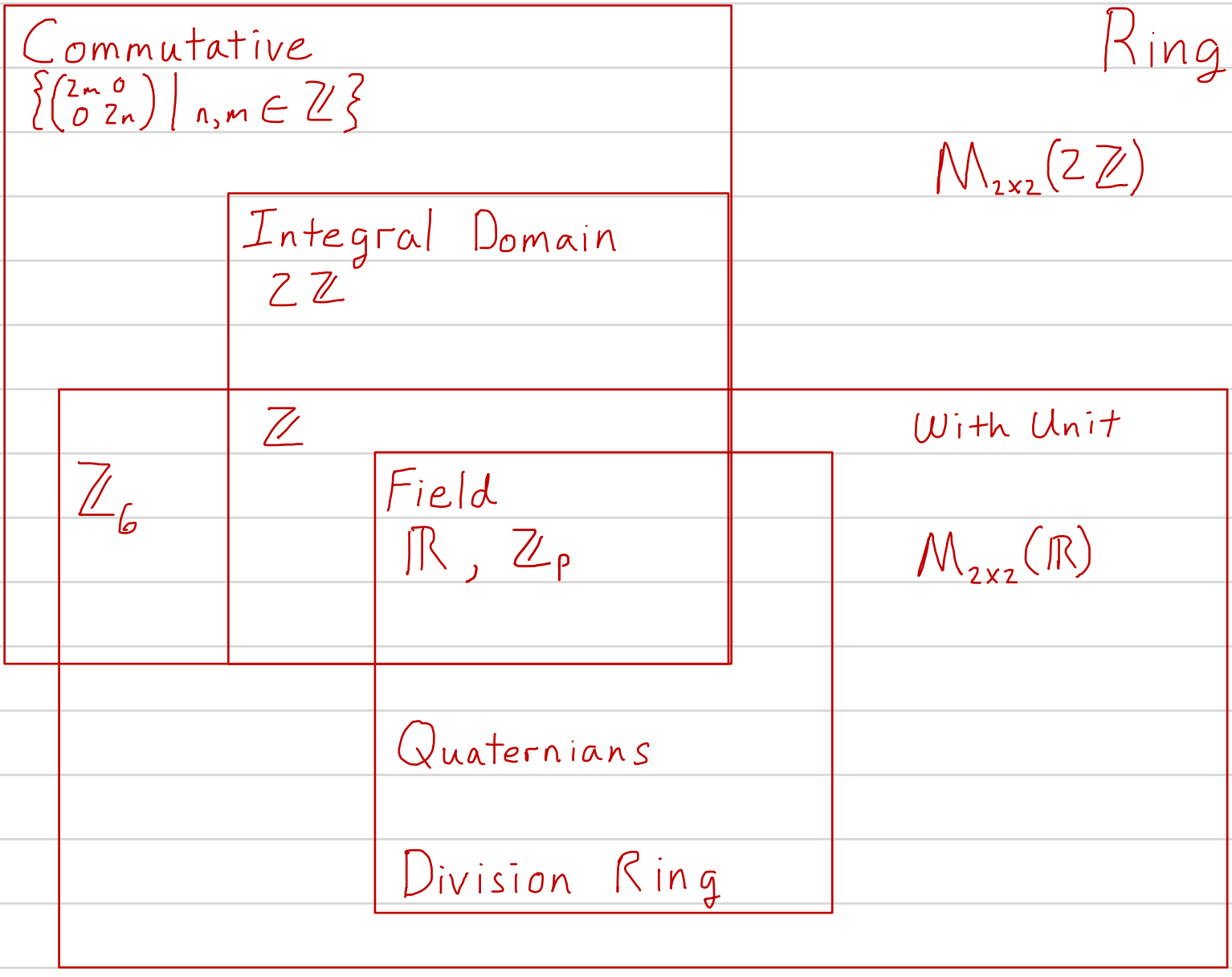
Note: If given a in a ring R there exist a^{-1} so that

$$a \cdot a^{-1}=a^{-1} \cdot a=1$$

then a is not a zero divisor.

Pf/ $a \cdot b=0 \Rightarrow b=a^{-1} \cdot 0$

$\Rightarrow b=0$ ∎



Lemma: Every finite integral domain is a field (p. 127 Herstein)

$R = 2 \cdot \mathbb{Z}_6 = \{0, 2, 4\}$

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

X	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

So 1 is not in the set, but there is a multiplicative identity

Corollary: $\mathbb{Z}_p$ is a field.

Definition of the Characteristic of an integral domain.

If $\forall m \in \mathbb{N}$ and $a \in R$ $m \cdot a = a+a+\cdots+a \neq 0$, Characteristic 0.

If $\exists m \in \mathbb{N}$ $\forall a \in R$ s.t. $m \cdot a = 0$, Characteristic m.

$\mathbb{Z}[x]$ vs $\mathbb{Z}_2[x]$.

Homomorphisms: $\varphi(a+b) = \varphi(a) + \varphi(b)$

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Ex 1: $\varphi(a) = a$: identity homomorphism

Ex 2: $\varphi(a) = 0$: trivial homomorphism

Ex 3: $\varphi: \mathbb{Z} \to \mathbb{Z}_n$

$\varphi(a) = a \pmod n$ [the remainder when a is divided by n]

Ex 4: $\varphi_r: R[x] \longrightarrow R$

$\varphi_r(f(x)) = f(r)$

$\varphi_r(f(x)+g(x)) = f(r) + g(r) = \varphi_r(f(x)) + \varphi_r(g(x))$

$\varphi_r(f(x) \cdot g(x)) = f(r) \cdot g(r) = \varphi_r(f(x)) \cdot \varphi_r(g(x))$

~Ex: $d: \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$

$d(f(x)) = f'(x)$

$d(f+g) = f' + g' = d(f) + d(g)$

$d(f \cdot g) = f \cdot g' + g \cdot f' \neq d(f) \cdot d(g)$

Definition: A subset U of a ring R is an ideal if

(1) U is a subgroup of the additive group R

(2) $\forall a \in U$ and $\forall r \in R$ ar and $ra \in U$.

Definition: $I(\varphi)$ = Kernel of $\varphi = \{r \mid \varphi(r) = 0\}$

Lemma: The Kernel is an ideal.

The basic roll of ideals for rings is the same as normal subgroups.

Look at 3.4 on your own.

Examples: $R = \mathbb{Z}$, $R_n = \mathbb{Z}_n$

$W = p\mathbb{Z}$, $U = n\mathbb{Z}$ in $\mathbb{Z}$

W' = multiples of p in $\mathbb{Z}_n$, $p|n = p\mathbb{Z}_n\ (p|n)$

$\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}_n/p\mathbb{Z}_n\ (p|n)$